

"Express Mail" mailing label number

EM091692683US

POINTING DEVICE WITH BIOMETRIC SENSOR

David J. Kinsella

CROSS-REFERENCE TO RELATED APPLICATION

This application claims the benefit under 35 U.S.C. § 119(e) of U. S. Provisional Application Serial No. 60/027,254 filed September 30, 1996, entitled "Controller Device" and naming David J. Kinsella as inventor, which provisional application discloses an exemplary embodiment of the present invention, and which provisional application is incorporated herein by reference in its entirety.

BACKGROUND OF THE INVENTION

Field of the Invention

This invention is related to pointing devices, and more particularly to such devices providing biometric feedback to an attached electronic system.

Description of Related Art

Modern society demands that people may be identified for many reasons. These include limiting access to bank accounts, limiting access to certain facilities such as a security area, a computer room, a police department, or a military facility, limiting which people are authorized to pick up a child from a day care center, limiting access to government welfare checks and health benefits, determining which prisoner to parole, and limiting access to adult activities such as electronic gambling. This has led to increasing use of identification cards, passwords, and PIN numbers to supplement, in those instances where automated identification is either necessary or desirable, those situations where human recognition is either unavailable or will not suffice. This obviously results in an increasing array and assortment of various cards, passwords, and PIN numbers that active participants in today's increasingly electronic

society must carry with them (or ideally must memorize) to be able to access the functions and capabilities requiring such identification and verification.

Biometrics is the study of biological phenomena, and in the area of personal identification, some chosen characteristic of a person is used to identify or verify that person's identity. Biometric identification has gained interest in recent years because certain personal characteristics have been found to be substantially unique to each person and difficult to reproduce by an impostor. Further, the recording and analysis of biometric data is generally susceptible to automation owing to the increased use of computer controlled electronics and digital recording techniques. Biometric systems are automated methods of verifying or recognizing the identity of a living person on the basis of some physiological characteristic like a fingerprint or iris pattern, or some aspect of behavior like handwriting or keystroke patterns.

The biometric identifying characteristic may be biologically determined as with a fingerprint, or it may be some characteristic that is learned or acquired, such as handwriting or voice patterns. Ideally, the characteristic should be unique for every person and unvarying over the time frame during which the person may be tested for identification. The characteristic should also be difficult to duplicate by an impostor in order to secure against erroneous identification.

Some of the biometric characteristics most investigated today for use in a personal identification system include fingerprints, hand or palm prints, retina scans, signatures and voice patterns. Hand or palm print techniques typically evaluate the shape of a person's hand or other significant features such as creases in the palm, but these techniques may be fooled by templates or models of the hand of an authorized person. Retina scanning techniques evaluate the pattern of blood vessels in a person's retina. A drawback of this technique is that the blood vessel pattern may vary over time, e.g., when alcohol is in the blood stream or during irregular use of glasses or contact lenses. Also, a user may feel uneasy about having his or her eye illuminated for retina scanning or the possibility of eye contamination if there is contact between the eye and the scanning apparatus. Signatures can be forged easily and must usually be evaluated by a human operator, although work has been done on automated

systems that evaluate the dynamics of a person's handwriting, such as the speed and the force of hand movement, pauses in writing, etc. Using voice patterns as the identifying characteristic encounters difficulties owing to the wide variations in a person's voice over time, the presence of background noise during an evaluation and the potential for an impostor to fool the system with a recording of the voice of an authorized person.

The most commonly used biometric characteristic and the one that has been the most investigated and developed is, of course, the fingerprint. Up until now, the technology of personal identification through fingerprint analysis has been used mainly in law enforcement, and this long term experience with fingerprint analysis has developed a large amount of information about fingerprints and has confirmed the uniqueness of a person's fingerprints. Historically, in law enforcement, fingerprints have been recorded by inking the fingerprint and making a print on a card for storage.

A fingerprint identification system is described in an article entitled "Vital Signs of Identity" by Benjamin Miller (IEEE Spectrum, February 1994, pp. 22-30). The system for recognizing fingerprints requires the user to press a finger onto a glass or Plexiglas platen. Image sensors under the platen and a charge-coupled device (CCD) array capture the fingerprint image. A custom computer system and software analyses the digitized image and converts it to an approximately 1K mathematical characterization which is compared against data stored in the local terminal or in networked versions of the system in a remote personal computer.

Rather than requiring a user to explicitly engage with verification devices, transparent verification attempts to identify the identity of a user not only unobtrusively, but during a transaction and using normal user interactions with the system. For example, a voice recognition system which also is able to identify a user by his voice pattern provides a capability of identifying a user as the user is speaking a request or command to the system, rather than as an explicit identification action or request by the user.

U.S. Patent No. 5,229,764 to Matchett et al. describes a continuous biometric authentication matrix. This system activates and analyzes the biometric data from a plurality of biometrically-oriented personal identification devices at intermittent intervals and selectively allows or prevents continued use of a particular protected system or device by a particular individual. The system acts as a continuously functioning gate between a system to be protected and a prospective user. Many of the biometrically-oriented personal identification devices in the Matchett system attempt some degree of transparent verification and include thumbscan, digital photo, voice prints, fingerprints and others. One such device is a joystick device shown in Figure 7 incorporating a thumbscan sensor on the top end of the joystick. In Figure 8A a computer mouse is depicted carrying a hand geometry reader in a mouse casing. The hand geometry reader is wired through the mouse and its leads run back to the rest of the scanning unit along the same conduit PG as that of the mouse. Figure 8B depicts a mouse having a thumbscan unit sensor incorporated into its side. The thumbscan sensor may be oriented relative to a mouse casing adapting it either for right-handed persons or left-handed persons or both. A mouse lead is modified or replaced to carry both the mouse data and the sensor data.

A pointing device such as a computer mouse, joystick, or trackball, includes two principal components: a positional indicator allows movement by a user to be communicated as user positional information to an attached system (e.g., a computer system) to allow, for example, a pointer to be moved around a window or a screen of a graphical user interface; and input switches or buttons so that a user can provide selection information to the system which corresponds to a particular location to which the positional indicator has been moved. Both kinds of information are communicated through a typically small cable to the system to which the pointing device is attached. Alternatively, infrared beams and RF interfaces have also been used to allow for wireless pointing devices, particularly a wireless mouse.

Notwithstanding these devices, there is a need for additional and improved verification devices and capabilities for electronic systems, particularly those

verification devices that provide for transparent continuous verification during normal user interactions with the system.

SUMMARY OF THE INVENTION

The present invention includes a pointing device which incorporates a biometric sensor at a location such that when operating the pointing device in a normal manner, a user's hand rests naturally in a position to place a finger of the user's hand in proximity to and readable by the biometric sensor. The location of the biometric sensor is equally well suitable for use by either a right-handed or a left-handed user, irrespective of hand size. Along with positional information from a position sensor and user selection information from at least one user-depressable button, the pointing device of the present invention also conveys to an attached system information associated with the user's identity detected by the biometric sensor. In one embodiment, the biometric sensor is a fingerprint sensor. Such a pointing device is well suited to both transparent verification as well as continuous, real-time verification, for if a user removes his or her hand from the natural position when using the device, the user's fingerprint will no longer be detectable by the fingerprint sensor, and the attached electronic system can be alerted as to the need to re-authenticate any additional attempts at using the pointing device. Minimal technical knowledge is required, for the identification functions are incorporated into a familiar pointing device. It affords a virtually foolproof, easily-used, and immediate method of identifying a user desiring access. A system audit log which records all attempted transactions, both authorized as well as non-authorized, may be easily implemented.

In one embodiment of the present invention, a pointing device includes an interface for operably communicating with an electronic system, a position sensor, responsive to user movement thereof, for conveying user positional information by way of said interface to the electronic system, a user-depressable button for conveying user selection information by way of said interface to the electronic system, and a biometric sensor disposed at a location such that when operating said pointing device in a normal manner a user's hand rests naturally in a position to place a finger of the

Figure 5 is an electrical block diagram of an embodiment of electronic circuitry useful within the computer pointing device shown in Figure 1.

Figure 6 is an electronic schematic drawing of interface circuitry depicted in Figure 5.

Figure 7 is an electronic schematic drawing of user-button circuitry depicted in Figure 5.

Figure 8 is an electronic schematic drawing of video circuitry depicted in Figure 5.

Figure 9 is a block diagram of a system incorporating the computer pointing device shown in Figure 1.

The use of the same reference symbols in different drawings indicates similar or identical items.

DESCRIPTION OF THE PREFERRED EMBODIMENT(S)

Trackball Embodiments

Figure 1, Figure 2, and Figure 3 illustrate a top view, a side view, and a rear view, respectively, of a trackball embodiment of the present invention. Referring specifically to Figure 1, a computer trackball pointing device 10 includes a base 12 which is substantially circular in shape and has a generally circular perimeter 14. It is preferably approximately 6 inches in diameter, weighs approximately 2 pounds, and is constructed generally of heavy duty plastic, although other dimensions are plausible. A chamfered surface 25 is formed between the top surface of base 12 and the perimeter surface 14. A trackball 16 is mounted off-center on the base 12 within a housing 28 formed on the base at a location intersecting the generally-circular perimeter surface 14. An upper section 18 is connected to the base 12 and includes, for this embodiment, three user-depressable buttons 22A, 22B and 22C formed substantially on a top surface 24 of the upper section 18. An interface 20 connects between the computer trackball pointing device 10 and an attached computer system,

or other electronic system. A fingerprint sensor (not shown) or other suitable biometric sensor is mounted, for this embodiment, below the center button 22B within the upper section 18 which is a location such that when operating the trackball pointing device 10 in a normal manner, a user's hand rests naturally in a position to place the second finger of the user's hand (i.e., the "middle" finger) in proximity and readable by the fingerprint sensor located below user depressable button 22B. The arrangement is well suited for all users regardless of hand size. The trackball pointing device 10 is adaptable for both right-handed and left-handed users because the upper section 18 is rotatably connected to the base 12 so that the trackball is positionable to either a position leftward or a position rightward of the upper section. The axis of this rotation is indicated at location 27 and provides for a symmetrical positioning of trackball 16 on either the left side or the right side of upper section 18.

Referring now to Figure 2, the bottom surface 30 of the base 12 is substantially flat and may include cushioning pads (not shown) such as low-profile self-adhesive rubber feet, or some other non-scratching surface treatment. The top surface 24 of the upper section 18 is shown, for this embodiment, as a substantially uniformly curved, convex surface which provides a comfortable surface for a user's palm and lower finger regions to rest comfortably upon the computer trackball pointing device 10. Referring specifically to the read view shown in Figure 3, the interface 20 is shown as a cabled interface passing through the rear surface of the upper section 18. The flat bottom surface 30 of base 12, particularly when implemented with a reasonable large diameter, allows the computer trackball pointing device 10 to easily be placed on a user's lap, or on a soft surface such as a bed, rather than requiring a hard surface such as a desktop.

To rotate the position of the trackball 16 from one side to the other, the computer trackball pointing device 10 is elevated from the surface upon which it rests, the upper section 18 is maintained in a direction pointing away from the user (the interface 20 pointing away from the user) and the base 12 is rotated upon axis 27 sufficiently to cause the trackball 16 within housing 28 to be moved from, for

- 9 -

3

other biometric sensor is located below a particular one of the button positions.

Figure 1 shows an pointing device 10 having three button positions, each of which is depicted to illustrate an operable button (e.g., buttons 22A, 22B, and 22C) at each of the button positions, but a particular button position may have either an inoperable button at such a location or no button whatsoever at the location. Moreover, the fingerprint sensor 44 or other biometric sensor may be located below a button position, whether operable or not, or at a location not beneath a button position. In another embodiment a three-button mouse includes a fingerprint sensor 44 disposed beneath an operable or inoperable center button position as is similarly depicted within the upper section 18 of the computer trackball pointing device 10 shown in Figure 1.

While the base of the computer trackball pointing device 10 is shown in Figure 1 as being rotatably connected to the upper section 18, other variations are equally plausible. For instance, a fixed connection could be easily implemented as a single-piece construction and could be configured for a right-handed or a left-handed user rather than as a single device which provides equal suitability to either a right-handed or a left-handed user. Likewise, similar moveable connections rather than a rotational connection are also contemplated which would allow a trackball device to be positioned in at least one of two locations such that suitable use for both right-handed and left-handed users may be achieved. The interface 20 which is depicted in Figure 1 as being a wired interface may also be implemented as a wireless interface and could include an infrared, a radio frequency or any variety of other wireless techniques. The interface may instead include a wireless interface having a transducer located at a rear surface of the upper section 18. Fingerprint sensor 44 may be implemented as an optical imaging array as depicted in Figure 4 in which the user's fingerprint is imaged through a transparent material forming button 22B. Such optical imaging arrays are commercially available, including from Suni Imaging Systems, Mountain View, California, and from Keytronics, Washington, D.C. Alternatively such a fingerprint sensor 44 may also be implemented as a capacitive imaging array, such as the FingerLoc™ series of sensors, available from the Harris Corporation, Melbourne, Florida.

Figure 5 is an electrical block diagram of one embodiment of an electronic sub-system 50 which may be implemented within the computer trackball pointing device 10 shown in Figure 1. The sub-system 50 includes an interface 51 which communicates to an attached computer system or other electronic system, a controller 55 for general control functions and for implementing traditional computer "mouse" functions, a button block 52 which includes traditional computer mouse user-depressable buttons, a pointer 53 which, in this case, includes circuits for implementing a computer trackball pointing device, and CCD camera 54 which provides a capability of visually scanning a user's fingerprint.

The interface 51 includes a group 60 of wires which provides communication to and from an attached system. These wires are preferably implemented using an unshielded twisted pair (UTP) cable having three twisted pairs of wires for connecting, using suitable connectors, to an attached computer or other electronic system. The group 60 of wires includes power terminal RAW12 and ground terminal GROUND for receiving power and ground from the attached system, differential video signal lines VIDEO+ and VIDEO- for conveying a differential video signal to the attached system, and serial data lines DATA and DATA_RET for respectively conveying serial data to and from the attached system. In other embodiments, a wireless interface, such as an infrared or RF interface, may also be used. On-board batteries may be used to power the pointing device in lieu of power cables.

The button block 52 includes three user-depressable buttons (not shown) and conveys a signal for each button (BUTTON1, BUTTON2, and BUTTON3) in a group 57 of wires to the controller 55. Other numbers of buttons are also possible, including one, or two. The pointer 53 includes the trackball position sensor and communicates positional information using signals X_CLK, X_DIR, Y_CLK, and Y_DIR to the controller 55 via the group 56 of wires. The pointer 53 may also include a computer mouse position sensor. Power is also received from the interface 51 via a wire within the group 56 of wires.

The controller 55 receives power from the interface 51 via one of the wires 56, and also sends and receives serial data to/from the interface 51 via wires 59 and 58,

respectively. Controller 55 provides for a point-and-click selection capability and data transfer capability to an attached system, to provide the traditional capabilities associated with a computer mouse or trackball.

Biometric sensor 54, such as a CCD camera, receives power from the interface 51 and conveys (for this example) a video signal to the interface 51 via wire 60. In other embodiments, other types of biometric sensors may be used, such as an capacitive fingerprint sensor rather than an optical sensor. One such sensor is the FingerLoc™ series of capacitive imaging array sensors, available from the Harris Corporation, Melbourne, Florida. Additional control and data signals (not shown) between the interface 51, the controller 55, and the biometric sensor 54 are to be expected in other embodiments.

Referring now to Figure 6, one embodiment of the interface 51 includes a voltage regulator 70 for generating a +5 volt power supply from an incoming +12 volt supply, along with various related filtering capacitors and a ferrite bead. Twin video amplifiers 71, 72 produce a differential video signal from a single-ended signal received from the biometric sensor 54. Video amplifier 71 is configured as a unity gain amplifier with a 75 ohm output impedance, and video amplifier 72 is configured as a negative unity gain amplifier, also with a 75 ohm output impedance. Serial data buffers 73, 74 provide simple buffering to an already serial signal received from the controller 55 (e.g., HDATA_OUT) or received from the attached system (e.g., HDATA_IN).

Figure 7 depicts one embodiment of the button block 52. A respective pull-up resistor to a +5 power supply voltage is momentarily connected to ground by a respective user-depressable switch, and which generates the respective button signal.

Figure 8 illustrates one embodiment of a biometric sensor 54 incorporating a CCD camera system which may be implemented within a pointing device, such as within the computer trackball pointing device 10 shown in Figure 1.

System Embodiments

Figure 9 illustrates a system 200 which includes a user interface terminal 202 connected via a connection 210 to a computer verification system 212. User interface terminal 202 includes a biometric input device 203 (e.g., a computer trackball pointing device 10), a keyboard 206, a display 204, and an interface controller 208. The computer verification system 212 includes an interface controller 214, a processor 216, and memory 218. The processor 216 generates an access control signal 220 when user identification and/or authorization has been confirmed and access to a particular system or feature (not shown) is warranted. Such an access-controlled system may reside within the computer verification system 212, or may be external to the computer verification system 212, and may include access to physical equipment or electronically stored or transmitted information.

Memory 218 includes known user storage 226 for storing the identification information, such as a fingerprint "signature," of users already known to the system 212. Memory 218 also includes authorization profile storage 222 for storing authorization information (e.g., permissible dates / times / functions / transactions / machines) for each user already known to the system 212. Memory 218 also includes an audit log storage 224 for storing successful and unsuccessful system accesses, as well as transaction information for users who successfully gain access to the system. The authorization profile storage 222, audit log storage 224, and known user storage 226 may be implemented together as one or more digital memory devices, or may be implemented using separate memory technologies, such as writable CDROM, magnetic disk, optical disk, flash memory, and other well known technologies. Advantageously, one or more of the authorization profile storage 222, the audit log storage 224, and the known user storage 226 may store encoded information, and may be implemented as an electronic memory device connected to the system 212, such as a removable PC card memory device. This affords, for example, an authorized user to carry his profile in a removable device and allows gaining access to any system to which the removable device is connected.

000050-2372560

A user initializes the verification system by first using the biometric input device 203, such as the computer trackball pointing device 10, to sense the biometric information (in this example, a fingerprint), to digitize it, optionally compress it or otherwise extract a "signature" representative of that user's fingerprint, and store the information, along with other user identifying information, into the known user storage 226. The stored "signature" is then used to identify and/or verify subsequent attempted accesses of the system 200.

Additionally, information is stored into authorization profile storage 222, preferably by one who controls access to the system, such as a system administrator, a hotel cashier, or others, to specify which user may perform which transactions at what times and dates, etc. Thereafter, when a user attempts to access the system, his or her fingerprint is read by device 203, and compared with the known user storage 226 and the authorization profile storage 222 to determine whether to allow the particular user to perform the function requested. If so, the processor 216 then drives the access control signal 220 and logs the particular transaction, time, date, and identification information for the user. The identification of the user is verified continuously as long as the user is in contact with the biometric input device 203 (for this example, the computer trackball pointing device 10). Each time the user inputs a system request, the verification process must be completed and maintained prior to continuing the use of the device being accessed. Verification times of several seconds are achievable with available processors and algorithms. If the use of the accessed device is discontinued, the verification process must be completed once prior to gaining access to the desired device, and use must be maintained for continued access.

If, at any time, a biometric reading is taken which does not match any user having a profile stored in the known user storage 226, access is denied and an audit log may be stored within the audit log storage 224 to provide a record of unsuccessful access attempts. Such an audit log entry may include time, date, attempted transaction, and a copy of the user identification information determined by the biometric device, such as a scanned fingerprint image, a fingerprint minutia representation, or others. Alternatively, if the user identifying information from the

biometric device is matched with a user found in the known user storage 226, but the authorization profile storage 222 indicates that the particular user has requested something for which he or she is not authorized, then access is also denied and an audit log entry is also created in the audit log storage 224. This entry may include time, date, attempted transaction, and an indication of the user's identity, such as a name, a photographic image, or others.

Such an audit log affords a significant capability to detect internal fraud and other unauthorized use by persons known to the system, and indeed authorized to perform some tasks, but not authorized for the task or function at the attempted time or date. For example, assume the system 200 is configured to provide access control to a cash register machine. Assume Sally and Mary are both registered employees known to the system and each has an entry in the known user storage 226. Further assume that Mary is continuously and properly verified during her shift as being authorized to engage in the type of transactions normally performed at her cash register. But if, during one of Mary's short work breaks, Sally tries to access the cash register during a time she is unauthorized, the system logs her unsuccessful attempt along with her name, picture, fingerprint, or some other identifying information. If Sally is unknown to the system altogether (i.e., no entry in the known user storage 226), then the audit log created may include, as well, as much identifying information, such as a fingerprint image, as possible to help law enforcement officials or others in identifying the person responsible for the unsuccessful access.

The computer trackball pointing device 10 may generate a scanned image of a users fingerprint, which is communicated to a host system for verification processing. Alternatively, the verification capability may reside within the computer trackball pointing device 10 along with authorized user keys to allow the pointing device to determine whether a user is authorized, without significant data transfers between the computer trackball pointing device 10 and the attached system. For example, the FingerLoc™ series of devices, available from the Harris Corporation of Melbourne, Florida, includes a down-loadable local memory for storing fingerprint profiles for up to 100 users, and includes a processor for independently determining whether an

observed fingerprint matches one stored within the local memory, without intervention from an attached host processor. In such an embodiment, the computer trackball pointing device 10 may therefore include biometric identification software, as well.

Combined Identification/Substance Detection Embodiments

In some embodiments of a pointing device employing an optical scanning capability, such as a color CCD imager, it may be possible to determine the blood alcohol content of the user simultaneously with scanning the fingerprint to determine the identification of the user. Such a combined identification/sobriety sensor would only allow access to an authorized person if he/she was sober. This could have tremendously beneficial applications in security access to military bases, power plants, industrial machinery areas, employer liability concerns, and others. A sensitive patch material is commercially available which, when in contact with a person's skin, changes color in response to chemical variations in the user's perspiration, and which is correlated to the person's blood alcohol content. A small patch of such material, if placed over the transparent window, allows a user's finger to be partially visible (and the patch could be sized small enough to preserve enough fingerprint information) for identifying a person, and yet still be large enough to sense perspiration variations, and change color appropriately enough to determine the blood alcohol content of the user. Such an arrangement would make the combined identification/sobriety sensor difficult for two people to fool. If the "authorized" person was drunk, and another person, a "thief," was sober, the system would still be hard to defeat. Such a system may be hard enough to defeat to permit unattended sobriety/identification terminals, for remote access control which ensures a sober user, not just an authorized user. Materials which may be used to detect other substances than alcohol, such as cocaine or other narcotics, may also be available and incorporated advantageously as described above.

Ten Finger Identification With Single Sensor

A pointing device such as a computer trackball pointing device 10 as shown in Figure 1, or any other device which has only one fingerprint sensor, may be used with up to all ten fingers to decrease the statistical chance of authentication error. For example, a user during the initialization sequence may be requested to place each of his/her fingers on the single fingerprint sensor so the system may learn each of the user's ten fingerprints. Then, periodically or at random, frequent intervals, the user may be requested by the system to place a certain finger on the sensor before the system proceeds. Also, such a system may request all ten fingers be presented sequentially to the sensor after a predetermined period of inactivity. The system may also demand all ten fingers be sequentially placed upon the fingerprint sensor before granting initial access, or after a predetermined period of user inactivity.

Foot-Print Embodiment

Embodiments of the present invention may include adaptations which allow a foot-operated pointing device which identifies a user by matching foot prints. A position sensor may be implemented in a much larger size to be easily operable with one or both feet, while large user-depressable buttons may be engaged with one or more toes, during which time one or more sensors scans portions of the user's foot or feet.

Other Embodiments

It should be appreciated that a mouse position sensor may be used instead of a trackball position sensor by using the teachings of this disclosure.

A fingerprint sensor may also be placed below a transparent trackball to allow reading a user fingerprint through the trackball. Distortions caused by the curvature of the trackball may be accounted for by software transformations of scanned fingerprint image data, or by merely "teaching" the fingerprint of an authorized user by using the same distorted optics.

